Ghost 后数据恢复的研究与实现

陈培德,吴建平,王丽清
(云南大学 信息学院 云南省高校数字媒体技术重点实验室,云南 昆明 650223)

摘 要:Windows 用户在使用 Ghost 工具软件安装操作系统时,有时会将“选择镜像文件到分区”误操作为“选择镜像文件到磁盘”;操作完成后,整个硬盘成为一个大 C 盘,造成各逻辑盘丢失。针对这一情况,以 Ghost8.0 为实验软件,Windows 7 为平台,WinHex 15.08 为分析工具,对 Ghost 后硬盘中 MBR 分区结构进行分析,提出了两种恢复 Ghost 后硬盘分区的基本思路与方法。第一种是通过各逻辑盘的 DBR 所在扇区号和总扇区数,在硬盘 0 号扇区重建各逻辑盘的 MBR 分区表来恢复各逻辑盘;另一种是通过重建硬盘 0 号扇区扩展分区表来恢复各逻辑盘。实验结果表明:误 Ghost 后除第 1 个逻辑盘中前面的部分数据被覆盖后无法恢复外,只要恢复各逻辑盘的 MBR 分区表,后续逻辑盘中的数据均可完整恢复。通过实践表明,这两种恢复方法不仅实用而且方便、快捷。

关键词:Ghost;镜像文件;分区表;数据恢复
中图分类号:TP311.12 **文献标识码**:A **文章编号**:1673-629X(2017)01-0112-05
doi:10.3969/j.issn.1673-629X.2017.01.025

Research and Implementation for Data Recovery after Ghost

CHEN Pei-de, WU Jian-ping, WANG Li-qing
(Key Laboratory of Digital Media Technology of Universities and Colleges in Yunnan Province,
School of Information Science and Engineering, Yunnan University, Kunming 650223, China)

Abstract: When the Windows users install the operating system with the Ghost tool software to their computers, they should make wrong operation of "to disk from image" instead of "to partition from image". After having finished it, the whole hard disk partition changes into a big Drive C, leading to the result that the primary partition in hard disk and the logical disk have lost. To aim the case, Ghost 8.0 is used as the experimental software, and the Windows 7 as the platform, and WinHex 15.08 as the analysis tool to analyze the primary partition structure in the hard disk after Ghost. The two thought and methods are put forward for recovering the partition in the disk. The first one is to rebuild the MBR partition table in the 0 sector for very logic disk by the DBR's sector number and total sectors for very logic disk in DBR, to recover all data in every logic disk. The second is to rebuild the extension partition table in the 0 sector for recovery of all data in every logic disk. The results of experiments indicate that the part of data in the front of disk could not be recovered, and the other data in the behind disk would be recovered integrally with, if the partition table would be recovered. The practice demonstrates that the two methods are not only useful, but also quick and easy.

Key words: Ghost; image file; partition table; data recovery

0 引 言

Ghost 是目前较多使用的快速地在硬盘上安装操作系统,备份和恢复数据的一款工具软件[1]。它实现了 FAT16、FAT32、NTFS、OS2 等多种硬盘分区格式的分区及硬盘数据的备份和还原功能[2]。

在微软视窗操作系统广为流传的基础上,为避开视窗操作系统原始完整安装的费时和重装系统后驱动应用程序再装的麻烦,许多软件安装人员把自己做好的干净系统用 Ghost 来备份和还原[3]。为使操作简洁,其流程被一键 Ghost、一键还原精灵等进一步简化,它的易用很快得到了软件安装人员的喜爱[4]。将视窗操作系统 Windows XP、Windows VISTA、Windows 7 等软件与系统引导文件、硬盘分区工具等集成为一体,进一步进行配套,这样用户在需要重装系统时能有效且简便地完成系统的快速重装。然而,用户在使用 Ghost 软件安装系统时,由于操作不慎,会误将选择分

收稿日期:2016-03-23 **修回日期**:2016-06-29 **网络出版时间**:2017-01-04
基金项目:云南省科技创新强省计划项目(2014AB021);云南省高校数字媒体重点实验室开放基金项目(2015KFKT002)
作者简介:陈培德(1966-),男,工程师,研究方向为文件系统与数据恢复技术。

区操作为选择整个硬盘[5],导致安装系统后,只有一个分区,其分区的大小为整个硬盘的大小[6]。文中对 Ghost 后数据恢复进行了大量实验,发现 Ghost 后大部分数据可以完整恢复。

1　实验环境及实验素材准备

1)实验环境。

(1)操作系统:Windows 7;

(2)Ghost 版本:8.0;

(3)数据恢复软件及分析工具:WinHex 15.08。

2)制作目标盘实验素材。

(1)Windows 7 操作系统下,使用 Windows 7 的虚拟磁盘管理功能在 D 盘的根目录上建立一个名为 abcd1. vhd 的文件,文件大小为 20 GB。

(2)将 abcd1. vhd 文件附加为虚拟磁盘 1,分区类型为 MBR,并将磁盘 1 划分为两个分区,即主分区和扩展分区。主分区的大小为 3 GB,对应的盘符为 F:\;扩展分区大小为 17 GB,在扩展分区中再建立三个逻辑盘,即 G 盘、H 盘和 I 盘。将各逻辑盘进行格式化,磁盘 1 中各逻辑盘基本情况如下:

· F 盘,文件系统:FAT32,容量:2.93 GB;

· G 盘,文件系统:NTFS,容量:4.88 GB;

· H 盘,文件系统:NTFS,容量:5.86 GB;

· I 盘,文件系统:NTFS,容量:6.32 GB。

(3)分别在 F 盘、G 盘、H 盘和 I 盘中存储一些文件夹和文件。

(4)使用 WinHex 软件查看 0 号扇区的分区表为“00 20 21 00 0B 92 54 7E 00 08 00 00 00 0C 5D 00”和“00 92 55 7E 05 FE FFFF 00 C8 5D 00 00 28 22 02”,第 1 个分区表对应 F 盘,第 2 个分区表对应扩展分区。

(5)F 盘的基本情况为:已用磁盘空间:480 MB;可用磁盘空间:2.45 GB;总容量:2.92 GB。每个扇区的字节数:512,每个簇的扇区数:8;保留扇区:4 414;隐藏扇区:2 048;总扇区数:6 144 000;每个 FAT 表所占扇区数:5 985,已使用簇号:2 ~ 123 066;未使用簇号:123 067 ~ 765 953。

至此,Ghost 前的目标盘已制作完成。

3)制作源盘实验素材。

(1)使用 Windows 7 的虚拟磁盘管理功能在 D 盘的根目录下再建立一个名为 abcd2. vhd 的文件,文件大小为 500 MB。

(2)将该文件附加为磁盘 2;分区类型为 MBR,在磁盘 2 中建立一个分区,文件系统选择 FAT32,并将其进行格式化,使用 WinHex 查看 0 号扇区的分区表为“00 02 03 00 0B FE 3F 3E 80 00 00 00 00 88 0F 00”,所对应的盘符为 J 盘,J 盘大小为 497 MB。

(3)在 J 盘的根目录下连续存储一些文件和文件夹。J 盘的基本情况为:已用磁盘空间:213 MB;可用磁盘空间:279 MB;总容量:493 MB。每个扇区的字节数:512,每个簇的扇区数:8;保留扇区:6 218;隐藏扇区:128;总扇区数:1 017 856;每个 FAT 表所占扇区数:987;已使用簇号:2 ~ 54 555;未使用簇号:54 556 ~ 126 209。

(4)使用 Ghost 软件将 J 盘做成一个镜像文件,文件名为:abcd3. gho,镜像文件大小为 212 MB。

至此,Ghost 前的镜像文件已制作完成。

2　Ghost 前硬盘整体布局

Ghost 前,各逻辑盘在磁盘 1 中的分布情况如图 1 所示。

在磁盘 1 的 0 号扇区有两个分区,即主分区(对应的盘符为 F 盘)和扩展分区[6];在扩展分区中有 G 盘分区表和 H 盘链接项、H 盘分区和 I 盘链接项、I 盘分区[7]。各逻辑盘分区表情况如表 1 所示。

表 1　Ghost 前各逻辑盘和扩展分区情况

分区	存储扇区号	扇区偏移	分区表
F 盘分区表	0	01BE ~ 01CD	00 20 21 00 0B 92 54 7E 00 08 0000 00 0C 5D 00
扩展分区表	0	01CE ~ 01DD	00 92 55 7E 05 FE FFFF 00 C8 5D 00 00 28 22 02
G 盘分区表	6 146 048	01BE ~ 01CD	00 B2 75 7E 071C E0 FC 00 08 0000 00 40 9C 00
H 盘链接项	6 146 048	01CE ~ 01DD	001C E1 FC 05 FE FF FF 00 489C 00 00 88 BB 00
H 盘分区表	16 388 096	01BE ~ 01CD	00 3D C2 FC 07 FE FFFF 00 08 0000 00 80 BB 00
I 盘链接项	16 388 096	01CE ~ 01DD	00 FE FFFF 05 FE FF FF 00 D0 57 01 00 58 CA 00
I 盘分区表	28 678 144	01BE ~ 01CD	00 FE FFFF 07 FE FF FF 00 08 0000 00 50 CA 00

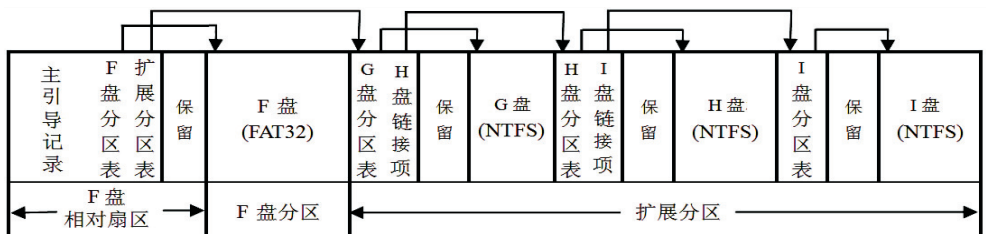

图 1　Ghost 前磁盘 1 各逻辑盘分布图

3 Ghost 操作步骤

以 Windows 7 操作系统为平台,使用 Ghost 软件以 abcd3. gho 为源文件,以磁盘 1 为目标盘,进行 Ghost 操作。

操作步骤如下:

(1) Local→Disk→From Image;

(2)从弹出的“Image File name to restore from”窗口中选择“abcd3. gho”;

(3)在弹出的“Select local destination drive by clicking on the drive number”窗口中选择目标驱动器—磁盘 1[6]。

4 Ghost 后硬盘整体布局

Ghost 后,各逻辑盘在磁盘 1 中的分布情况如图 2 所示。即在磁盘 1 的 0 号扇区建立了一个分区,主分区所对应的盘符为新 F 盘,新 F 盘的大小为整个磁盘 1 的容量。

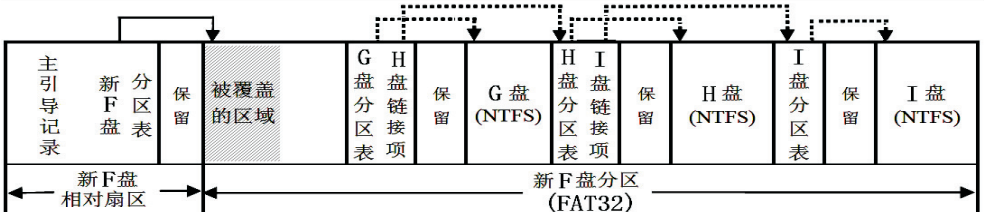

图 2 Ghost 后磁盘 1 布局图

从 Ghost 前和 Ghost 后对比图可知,Ghost 后,目标文件 abcd3. gho 只覆盖了 Ghost 前 F 盘的一部分数据,F 盘未覆盖的部分可以使用按文件名的形式进行恢复。G 盘、H 盘和 I 盘中所存储的文件夹和文件没有被覆盖,可以全部恢复。

注:Ghost 后,由于 0 号扇区的扩展表已删除,所以 G 盘分区表、H 盘链接项、H 盘分区表、I 盘链接项和 I 盘分区表已不再起作用,如图 2 中的虚线部分。其分区表情况如表 2 所示。

表 2 Ghost 后各分区情况

分区	扇区号	扇区偏移	分区表
F 盘分区表	0	01BE ~ 01CD	00 01 01 00 0C FE FF FF 3F 00 00 00 73 CB 7F 02
G 盘分区表	6 146 048	01BE ~ 01CD	00 B2 75 7E 071C E0 FC 00 08 0000 00 40 9C 00
H 盘链接项	6 146 048	01CE ~ 01DD	00 1C E1 FC 05 FE FF FF 00 489C 00 00 88 BB 00
H 盘分区表	16 388 096	01BE ~ 01CD	00 3D C2 FC 07 FE FFFF 00 08 0000 00 80 BB 00
I 盘链接项	16 388 096	01CE ~ 01DD	00 FE FFFF 05 FE FF FF 00 D0 57 01 00 58 CA 00
I 盘分区表	28 678 144	01BE ~ 01CD	00 FE FFFF 07 FE FF FF 00 08 0000 00 50 CA 00

5 数据恢复的方法与步骤

经过大量实验,发现对于 Ghost 后,可以通过两种方法来恢复数据:

方法一:

(1)恢复 G 盘、H 盘和 I 盘三个逻辑盘在 0 号扇区偏移地址 0X01CE ~ 0X01FD 的主分区表;

(2)调整新 F 盘分区表中的总扇区数(扇区偏移为 0X01CA ~ 0X01CD);

(3)调整新 F 盘 FAT32_DBR 中的总扇区数(扇区偏移为 0X020 ~ 0X023)。

完成以上操作就可以恢复 Ghost 前 G 盘、H 盘和 I 盘中的所有文件夹和文件;同时也可以查看新 F 盘的全部文件夹和文件。恢复后的各分区表与各逻辑盘分布图如图 3 所示。

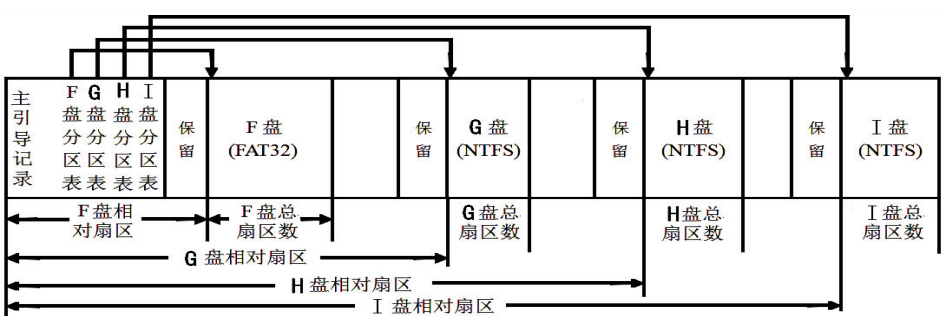

图 3 恢复后磁盘 1 中各逻辑盘的分布图

恢复步骤为:

(1)启动 WinHex 软件,通过 NTFS_DBR 的特征值(注:NTFS_DBR 的特征值为扇区前三个字节的值为“EB5290”[8])查找 NTFS_DBR 所在扇区号。

(2)分别在 6 146 048 号扇区、16 388 095 号扇区等找到;经确认各 NTFS_DBR 作用如表 3 所示。

表 3　磁盘 1 中 NTFS_DBR 和 NTFS_DBR 备份所在扇区号

盘符	NTFS_DBR 所在扇区号	NTFS_DBR 备份所在扇区号	所占扇区数
G 盘	6 148 096	16 388 095	10 240 000
H 盘	16 390 144	28 678 143	12 288 000
I 盘	28 680 192	41 938 943	13 258 752

(3)从表 3 可以计算出磁盘 1 中 Ghost 前 G 盘、H 盘和 I 盘在 0 号扇区的分区,如下所示:

· G 盘“00 01 01 00 07 FE FF FF 00 D0 5D 00 00 40 9C 00”

· H 盘“00 01 01 00 07 FE FF FF 00 18 FA 00 00 80 BB 00”

· I 盘 “00 01 01 00 07 FE FF FF 00 A0 B5 01 00 50 CA 00”

对 G 盘、H 盘和 I 盘分区表说明如下:

①由于 G 盘、H 盘和 I 盘均不引导系统,各分区表中第 1 个字节的值为“00”[9];

②目前硬盘的存取方式均为 LBA,分区表中第 2 ~4字节未定义,可以填充任意值,这里填充“01 01 00”[9];

③由于要恢复的逻辑盘的文件系统均为 NTFS,分区标志为“07”[10-11];

④分区表中第 6 ~ 8 字节未定义,可以填充任意值,这里填充“FE FF FF”[9];

⑤分区表中第 9 ~ 12 字节为相对扇区,即各逻辑盘 NTFS_DBR 所在扇区号;

⑥分区表中第 13 ~ 16 字节为总扇区数,即各逻辑盘所占扇区数[12]。

(4)调整新 F 盘分区表中的总扇区数,由于 G 盘 NTFS_DBR 所在扇区号为 6 146 048,所以可以推算出新 F 盘的结束扇区号为 6 146 047,而新 F 盘分区表中的相扇区为 63,所以新 F 盘总扇区数为 6 418 033。新 F 盘分区表为“00 01 01 00 0C FE FF FF 3F 00 00 00 C1 CF 5D 00”。

(5)将计算好的 3 个分区表填充 0 扇区偏移 0X01CE ~0X01FD 处,并将第 1 个分区表总扇区数(偏移地址为 0X01CA ~0X01CD)修改为“C1 CF 5D 00”。

(6)将光标移到 63 号扇区,即 F 盘 FAT32_DBR 所在扇区,将 F 盘 FAT32_DBR 中总扇区数(扇区偏移地址为 0X020 ~0X023)修改为“C1 CF 5D 00”。

(7)存盘并退出 WinHex,到资源管理器可以查看到恢复出来的 G 盘、H 盘和 I 盘中的文件夹和文件,以及新 F 盘中的文件夹和文件。

方法二:

(1)恢复 Ghost 前 0 号扇区的扩展分区表;

(2)调整 Ghost 后新 F 盘分区表中的总扇区数;

(3)调整新 F 盘 FAT32_DBR 中的总扇区数。

完成以上操作就可以恢复 Ghost 前 G 盘、H 盘和 I 盘中所有文件夹和文件;同时也可以查看 Ghost 后 F 盘的全部文件夹和文件。恢复后的各逻辑盘结构图如图 1 所示,即 Ghost 前的结构图。

恢复步骤为:

(1)启动 WinHex 软件,通过特征值来查找 G 盘分区表和 H 盘链接项所在扇区号(注:特征值为扇区最后两个字节的值为“55AA”[12])。

(2)在 6 146 048 号扇区找到,即扩展分区表的相对扇区为 6 146 048。

(3)由于整个硬盘的总扇区数为 41 943 041,可以估算扩展分区表的结束扇区号为 41 943 020,即扩展分区在整个硬盘中扇区号为 6 146 048 ~ 41 943 020,扩展分区中总扇区数为 35 794 925。

(4)扩展分区在 0 号扇区偏移 0X01CE ~ 0X01DD 处的分区表为“00 01 01 00 05 FE FF FF 00 C8 5D 00 EC 37 22 02”。

对扩展分区表说明如下:

①扩展分区表不引导系统,第 1 个字节的值为“00”;

②第 2 ~ 4 字节未定义,可以填充任意值,这里填充“01 01 00”;

③第 5 个字节为扩展分区标志位,取值为“05”或“0F”,这里取“05”[13];

④第 6 ~ 8 字节未定义,可以填充任意填,这里填充“FE FF FF”;

⑤第 9 ~ 12 字节为相对扇区,即 G 盘分区表和 H 盘链接项所在扇区号,其值为 6 146 048,在分区表中的存储形式为“00 C8 5D 00”;

⑥第 13 ~ 16 字节为总扇区数,即扩展分区表所占总扇区数,其值为 35 794 925,在分区表中存储形式为“EC 37 22 02”。

(5)由于在 6 146 048 号扇区找到 G 盘分区表和 H 盘链接项,确定新 F 盘的结束扇区号为 6 146 047。即新 F 盘所占扇区号为 63 ~ 6 146 047,分区表中总扇区数为 6 145 985,在分区表中的存储形式为“C1 C7 5D 00”;即新 F 盘的分区表修改为“00 01 01 00 0C FE FF FF 3F 00 00 00 C1 C7 5D 00”。

(6)将计算好的扩展分区表填入至 0 号扇区偏移 0X01CE ~ 0X01DD 处,并将第 1 个分区表总扇区数(扇区偏移地址为 0X01CA ~0X01CD)修改为“C1 C7 5D 00”。

(7)将光标移到 63 号扇区,即 F 盘 FAT32_DBR 所在扇区,将 F 盘 FAT32_DBR 中总扇区数(扇区偏移

地址为“0X020 ~0X023”[14])修改为“C1 C7 5D 00”。

(8)存盘并退出 WinHex,到资源管理器可以查看到恢复出来的 G 盘、H 盘和 I 盘中的文件夹和文件,以及新 F 盘中的文件夹和文件。

至此,Ghost 前的 G 盘、H 盘和 I 盘中所存储的全部文件夹和文件均已被完整恢复出来。如果要恢复的文件内容存储于原来 F 盘未被覆盖的区域,可以使用 WinHex 按文件类型功能进行恢复。

6 结束语

除使用 Ghost8.0 做实验外,还使用 Ghost11.0.1 做了大量实验。实验结果发现:Ghost 后,除被覆盖的区域外,还将 G 盘分区表、H 盘链接项、H 盘分区表和 I 盘分区表删除,只留下 I 盘链接项。对于这种情况,使用方法一来恢复更为方便一些,但方法一只能恢复 4 个分区表,如果分区多于四个可以先恢复四个分区,将各逻辑中的文件复制出来后,再通过修改分区表的形式恢复剩余分区中的文件夹和文件。

对于方法二,使用 Ghost11.0.1 后,如果 G 盘分区表、H 盘链接项、H 盘分区表和 I 盘分区表四个分区表被删除,只留下 I 盘链接项,这种情况的恢复思路如下:

(1)计算扩展分区表;

(2)计算 G 盘分区表、H 盘链接项、H 盘分区表和 I 盘分区表;

(3)计算 G 盘分区表和 H 盘链接项所在扇区号;

(4)计算 H 盘分区表和 I 盘链接项所在扇区号;

(5)计算 I 盘分区表所在扇区号;

(6)将扩展分区表填入至 0 号扇区偏移 0X01CE ~0X01DD 处,将 G 盘分区表和 H 盘链接项填入所在扇区偏移 0X01BE ~0X01DD 处,将 H 盘分区表和 I 盘链接项填入所在扇区偏移 0X01BE ~0X01DD 处,将 I 盘分区表填入所在扇区偏移 0X01BE ~0X01CD 处;

(7)调整 Ghost 后新 F 盘分区表中的总扇区数和新 F 盘 FAT32_DBR 中的总扇区数。

综上所述,Ghost 后整个硬盘分区变为一个大分区,恢复 Ghost 前逻辑盘中全部数据的核心工作在于重建分区表。

参考文献:

[1] 贺惠萍,荣 彦,张 兰,等. Windows+7 万能 Ghost 启动盘仿真软件的设计与实现[J]. 实验技术与管理,2014,31(5):127-130.

[2] 张钟澍,陈代军,李新萌. 修复和维护你的硬盘[M]. 北京:北京希望电子出版社,2002:298.

[3] 丁一钧. 利用 GHOST 重装操作系统疑难问题解析[J]. 电脑编程技巧与维护,2013(14):122-123.

[4] 杨海瑞. 试谈机房使用 Ghost 恢复系统的方法[J]. 电脑编程技巧与维护,2013(20):111-112.

[5] 陈培德,吴建平,王丽清. NTFS 文件系统实例详解[M]. 北京:国防工业出版社,2015.

[6] 刘 伟. 数据恢复技术深度揭秘[M]. 北京:电子工业出版社,2010.

[7] 马 林. 数据重现—文件系统原理精解与数据恢复最佳实践[M]. 北京:清华大学出版社,2009:43-51.

[8] Carrier B. File system forensic analysis[M]. [s. l.]:Addison Wesley Professional,2005:160.

[9] 汪中夏,张京生,刘 伟. RAID 数据恢复技术揭秘[M]. 北京:清华大学出版社,2010:102-115.

[10] 戴士剑,涂彦晖. 数据恢复技术[M]. 北京:电子工业出版社,2005:97.

[11] 刘乃琦,郭建东,张 可. 系统与数据恢复技术[M]. 成都:电子科技大学出版社,2008:46.

[12] Fathi B. 深入解析 Windows 操作系统(第 5 版 · 英文版)[M]. 北京:人民邮电出版社,2009.

[13] Hogan T. The programmer´s PC sourcebook[M]. USA:Microsoft Press,1988:60.

[14] Ivens K,Gardinier K. Windows 2000:the complete reference[M]. [s. l.]:McGraw-Hill Companies,2000:531.

(上接第 111 页)

[13] 任守纲,徐焕良,黎 安,等. 基于 RFID/GIS 物联网的肉品跟踪及追溯系统设计与实现[J]. 农业工程学报,2010,26(10):229-235.

[14] 梁正平,纪 震,林佳利,等. 基于三维编码的全流程食品追溯系统[J]. 深圳大学学报:理工版,2010,27(3):312-316.

[15] 邓方源,景小平. 基于物联网的低成本食品跟踪技术的应用研究[J]. 计算机科学,2011,38(10):26-29.

[16] 张 丽,余 华,马新明. 基于物联网的农产品质量安全信息系统平台[J]. 中国科学:信息科学,2010(S1):220-229.

[17] 邓小云,赖茂生. 基于云计算的食品安全监理研究[J]. 北京工商大学学报:自然科学版,2012,30(4):75-78.

[18] 刘光明,季延滨,孙学亮. 基于云计算的淡水鱼封闭循环式养殖平台设计[J]. 湖北农业科学,2015,54(11):2755-2757.

[19] 黎建辉,杨风雷,崔建业,等. 全球食品安全信息监控与分析云平台架构研究[J]. 计算机应用研究,2014,31(8):2361-2366.

[20] 刘 彤,谭 红,张经华. 基于大数据的食品安全与营养云平台服务模式研究[J]. 食品安全质量检测学报,2015(1):366-371.

[21] 王娟娟. 基于电子商务平台的农产品云物流发展[J]. 中国流通经济,2014(11):37-42.